UCRL-WEB-201524

Firewall and SSH Guide

Table of Contents

Preface

Scope: The Firewall and SSH Guide describes the user-relevant features of LC's security firewall that protects (some) machines in the llnl.gov domain, tells how to use indirectly the services (such as FTP) that the firewall blocks directly, and introduces alternative services (such as secure shell SSH and local variants, or Virtual Private Network VPN) intended to take the place of the blocked services. See the EZACCESS (URL: http://www.llnl.gov/LCdocs/ezaccess) guide for a comparative general introduction to the many ways to reach LC computing resources, of which access though the firewall is only one. See the EZSTORAGE (URL: http://www.llnl.gov/LCdocs/ezstorage) guide if you are primarily concerned about storing at LC project files that were generated elsewhere.

Availability: When the programs described here are limited by machine, those limits are included in their explanation. Otherwise, they run under any LC UNIX system.

Consultant: For help contact the LC customer service and support hotline at 925-422-4531 (open e-mail: lc-hotline@llnl.gov, SCF e-mail: lc-hotline@pop.llnl.gov).

Printing: The print file for this document can be found at:

```
on the OCF: http://www.llnl.gov/LCdocs/firewall/firewall.pdf
on the SCF: https://lc.llnl.gov/LCdocs/firewall/firewall_scf.pdf
```

Introduction

This document describes LC's security firewall. It tells how to continue using those services (such as FTP) whose normal behavior the firewall alters, and it introduces some alternative services (such as secure shell SSH) intended to take the place of the ones that the firewall blocks. See the EZACCESS (URL: http://www.llnl.gov/LCdocs/ezaccess) basic guide for a more general, comparative introduction to the many different ways to reach LC computing resources.

Because firewall terminology can be arcane, this introduction briefly explains some crucial terms and distinctions used later in the text. If you are already familiar with these background definitions, just skip directly to the sections about LC's specific firewall implementation and its effects on users. This document is NOT a general review of all known firewall tools and techniques, but rather practical advice for users coping with LC's particular firewall.

Data moves around computer networks in discrete packets (of bits), governed by standard rules (protocols). The well-known IP (Internet Protocol) delivers packets to intended destinations, fragmenting and reassembling messages as needed. The TCP (Transmission Control Protocol) performs error checking and handles packet retransmission if damage or loss occur. Each network "service" (such as TELNET or FTP) uses a numerical extension of the receiving machine's IP address (e.g., 134.9.55.51 for ILX1.LLNL.GOV) to keep track of packets associated with that service. This is often called a port number (e.g., 23 is the default port number for TELNET traffic). Upon this basis (of protocols and port numbers) firewall security is built.

The most basic firewall technique is PACKET FILTERING. Packet filtering usually takes place at a "screening router" located on the border of a network. The screening router examines incoming packets and decides whether to block them or allow their access to different machines on the protected network by consulting a (locally supplied) list of rules. These rules can allow or block network packets based on

- packet source,
- packet destination,
- IP protocol type, or
- TCP (or other) port number.

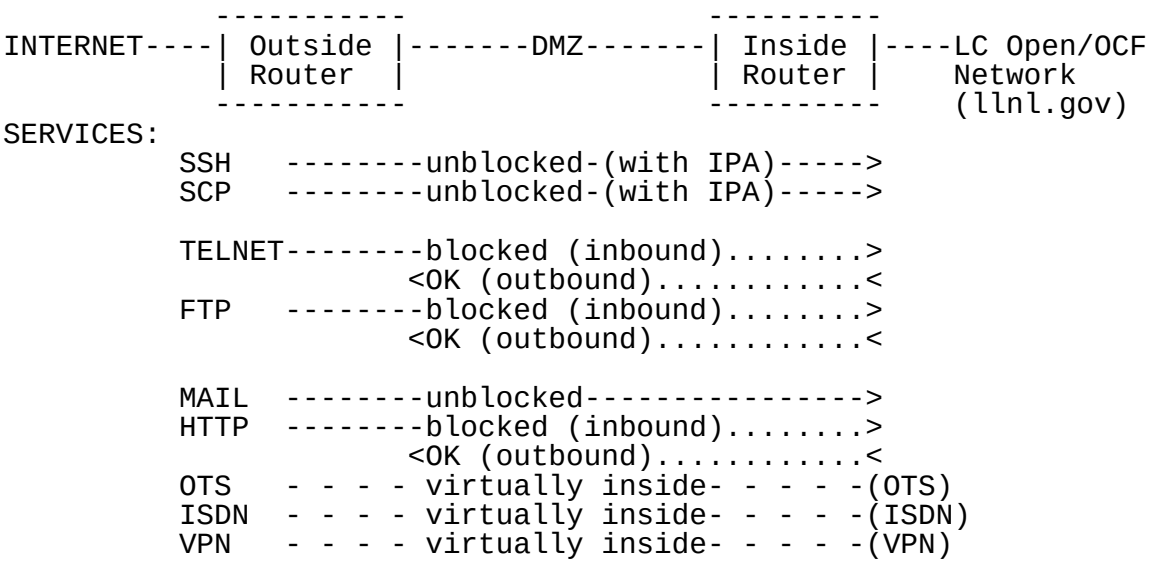
For example, one way to prevent anyone from TELNETing to your local machines is to block packets for TCP port 23 from coming through the filter.

A second, enhanced approach to firewall security involves PROXY SERVERS. A proxy server is software specific to each application or service (e.g., one for TELNET, a different one specifically for HTTP) that aims to prevent clients outside the protected network from DIRECTLY contacting servers inside the protected network (or, sometimes, vice versa). When a firewall incorporates proxy servers, each (outside) client makes requests to the (appropriate) proxy server, which then, if allowed by its (locally supplied) list of rules, indirectly retrieves the requested information from the real server and returns it to the client.

Firewall Features at LC

This section describes the design of LC's security firewall, explains how its features affect your access to LC computers, and summarizes the firewall's effect on each "service" (such as TELNET) that you might use. The next section (page 8) gives detailed instructions for using each service whose behavior the firewall has changed (blocked).

This diagram shows the LC firewall and its features, and suggests its effect on each relevant service (details follow):



The LC firewall consists of these FEATURES:

Outside Screening Router

performs packet filtering on incoming network traffic (i.e., on packets coming from the Internet toward machines on LC's own open (OCF) network). Some packets (those with TELNET or FTP port numbers) are completely blocked inbound. Other packets (e.g., those with SSH or SCP port numbers) pass through unblocked. Currently, incoming MAIL packets are also unblocked. OUTWARD packets (headed from LC's network toward the Internet) or travelling among llnl.gov machines are NOT affected by this router.

DMZ ("demilitarized zone") is a subnet between two screening routers where security-enhancing software resides on "bastion hosts." Examples include
(A) GATEWAYS that demand extra authentication before allowing a service (such as TELNET) to cross, or
(B) PROXY SERVERS that prevent any direct contact between clients and servers by catching and retransmitting only those packets that meet specified safety rules (for each different service).

Inside Screening Router

performs additional packet filtering on incoming network traffic. Packets with TELNET and FTP port numbers were formerly only allowed if they originated from an LC gateway within the DMZ (above), but this ended in April, 2000. SSH and SCP packets are allowed to continue from any source, as are (currently) MAIL. OUTWARD packets (headed from LC's network toward the Internet) or travelling among llnl.gov machines are NOT affected by this router.

The SERVICES that the LC firewall manages are individually controlled to achieve different security goals. The next section (page 8) gives detailed instructions for those services whose behavior the firewall has changed. The current security "stance" toward each service is summarized here (in the order shown on the diagram above):

SSH and SCP (secure shell and secure copy) are the preferred log-on and file-transfer services that the firewall allows inward (with prior IPA (page 20) authentication) from any source to any llnl.gov destination. SSH and SCP service outward from any supporting llnl.gov machine (and among LC machines) is also freely allowed. See the SSH (page 10) section below for advice on installation and use, including how to authenticate your SSH session with IPA.

TELNET inward to any LC llnl.gov machine from any machine outside llnl.gov as well as from any nonLC llnl.gov machine (i.e., from any machine outside the 134.n.n.n IP domain) is totally blocked. (TELNET service among LC machines themselves was also blocked in February, 2001.) TELNET service outward from LC (134.n.n.n-domain) machines to nonLC machines is still freely allowed. Former gateway support for inward TELNET access was discontinued in April, 2000.

FTP inward to any LC llnl.gov machine is totally blocked. FTP service outward from (or among) llnl.gov machines is freely allowed. Former gateway support for inward FTP access was discontinued in April, 2000. Running a VPN (page 24) client on your offsite computer before starting an FTP session sometimes avoids this blocking (see the FTP (page 9) section for details).

SFTP inward to any LC llnl.gov machine, including FIS, is totally blocked. Even using OTS or VPN will *not* enable SFTP access from offsite machines to FIS.

MAIL inward or outward moves freely through the firewall now (this may change later).

HTTP (World Wide Web service) has been split by locating some LLNL WWW servers outside the firewall while placing others behind it. The public servers remain available to all users (e.g., www.llnl.gov), but requests for the restricted servers are now blocked at the firewall. Running a VPN (page 24) client on your offsite computer before starting an HTTP (web-browser) session avoids this blocking.

OTS (Open Terminal Server) lies outside the LC firewall but is treated as if it were a local machine residing inside the firewall, so OTS users will see no service change.

ISDN	(fast telephone connection) lies outside the LC firewall but is treated as if it were a local machine residing inside the firewall, so ISDN users will see no service change.
VPN	(Virtual Private Network) is a pair of servers outside the firewall (vpn1.llnl.gov and vpn2.llnl.gov) that lets authorized users borrow an IP address from a domain behind the firewall so that (some) other offsite applications (such as web browsers and FTP, but not SFTP) can avoid the usual firewall service restrictions. See the VPN (page 24) section below for advice on installation and use.

Services Affected by the Firewall

This section tells how to continue using those services whose normal behavior is altered by the LC firewall (other services perform as if the firewall did not exist).

CRYPTOCard Use

Until April, 2000, some services whose direct use was blocked by the LC firewall could be used indirectly through a special security-enhanced gateway if you had an LC-issued "cryptocard" (also called an "authentication token card") to provide extra authentication. CRYPTOCards were recalled and their use with the gateway was discontinued in April, 2000. See the SSH (page 10) section below for the best current alternative.

TELNET

LC encourages offsite users to run secure shell SSH (page 10) instead of TELNET to log on to open-network LC machines. For this reason, LC's firewall allows SSH traffic from any outside host but totally blocks all TELNET traffic from every host outside the 134.n.n.n IP domain (that is, blocks all TELNET traffic from all nonLC hosts, including llnl.gov hosts outside the LC-controlled 134 IP domain). For a while, such "outside" users could obtain a CRYPTOCard for authentication (see the previous section (page 8)) and log on to the firewall gateway (gw-lc.llnl.gov), then open an (indirect) TELNET connection to any other LC machine. That exception ended in April, 2000. Similarly, TELNET traffic among LC machines themselves was blocked in February, 2001. Only client TELNET service outward from 134.n.n.n machines to other IP domains (such as UC's melvyl.ucop.edu) remains. See the SSH (page 10) section below for the best current alternative.

FTP

LC's firewall totally blocks all FTP traffic from every host outside the llnl.gov domain. To transfer files from machines outside llnl.gov to any LC machine, outside users have three choices:
(1) Log on to an LC machine first, then execute FTP on that machine and connect back to the outside machine where the sought files reside, using GET to retrieve them. This approach poses known problems for Macintosh files, and suggested solutions appear in the "Macintosh File-Transfer Problems" section of EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput). It also requires that an FTP server (not just a client) run on the outside machine, a problem for some workstations.
(2) Run secure copy SCP (also described in EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput)) instead of FTP to transfer files toward an open-network LC machine. You must have previously installed SSH on the outside machine (LC's firewall freely allows SSH and SCP traffic from any IPA-authenticated (page 20) outside host.)
(3) Run a VPN (Virtual Private Network) client on your outside machine before you start your FTP file-transfer session. VPN temporarily borrows an llnl.gov IP address for the machine where it runs, thus enabling other programs (such as FTP) to act as if they were running inside, not outside, the firewall. You must first get a VPN account, download the VPN client appropriate for your operating system, and configure it for use with LLNL's VPN server (instructions are in the VPN (page 24) section below). LC has confirmed that VPN enables inward file transfers with FTP (even to storage) when FTP and VPN run under Windows98, but you may encounter vendor-compatibility problems with other versions of Windows or with other operating systems.
(4) Former FTP access through a CRYPTOCard-authenticated gateway was discontinued in April, 2000.

FTP USAGE WARNINGS:

Storing Files.
LC's open file-storage system (HPSS) does NOT accept secure copy SCP connections. So offsite users who want to store files archivally in HPSS must either
(A) log on to some llnl.gov LC machine (such as ILX1) using SSH, execute FTP there and GET their remote files, then PUT those files from the LC machine into storage.llnl.gov, or
(B) use SCP to move their files to some llnl.gov LC machine (such as ILX1), and then (use SSH to) log on to that machine and execute FTP there to secondarily move the files again to storage.llnl.gov.

Anonymous FTP Service.
LC's own former anonymous FTP service resided on k2.llnl.gov and west.llnl.gov (neither machine exists now). Service moved to a machine located in the DMZ between the two screening routers of its firewall (ftp-lc.llnl.gov), then was discontinued altogether even for llnl.gov users. Anonymous FTP users both inside and outside llnl.gov must now instead contact the LLNL institutional anonymous FTP server at ftp.llnl.gov (where directory and file names may have changed, so check with the provider of your sought anonymous FTP files for details). A section in EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput) summarizes this service.

Secure FTP (SFTP).
SFTP connections (to FIS) work only from OCF machines within LC's firewall. Even using OTS or VPN will *not* enable you to connect from an offsite machine by running SFTP.

Secure Shell (SSH)

Role of SSH

The secure shell (SSH) is a product (for which there are public domain and licensed versions) designed to provide an easy, secure connection (over an unsecure channel) between two Internet sites. SSH, once installed and initialized on both the local and remote machines, allows you to

- log in to the remote computer,
- execute commands on the remote computer,
- move files between the local and remote machines (using SCP), and
- provide secure X connections.

SSH is intended to replace the less secure programs RLOGIN, RSH, and RCP, and it mostly shares their syntax. SSH has two prime security advantages over RSH and TELNET for between-machine connections:

- The data and control stream between SSH sites are enciphered to deter network packet sniffing. File transfers using SCP are fully enciphered too, but if you use FTP to "tunnel through" an SSH session to transfer files, only the control stream is encrypted, not the date stream.
- Strong authentication of both hosts and users is performed using robust "public-key" cryptography. No clear-text passwords are sent.

At LC, SSH packets pass unblocked through the firewall in both directions, while RSH has been discontinued and TELNET service is now blocked both from outside inward to, and internally among, all LC llnl.gov machines.

Starting on April 18, 2001, as an additional security measure, users outside the LLNL firewall (except for those on the restricted networks at SNL and LANL) must authenticate a (timed) session with IP Port Allow (IPA) before their SSH traffic will be allowed to reach LC target machines. See the IPA section (page 20) below for more background and for the needed IPA authentication steps. In October, 2001, all LC SSH servers on the open (OCF) network were modified to accept one-time passwords (OTP) from SSH clients.

Users concerned about slow performance (during graphics-intense sessions, for example) caused by the extra overhead of SSH encryption should consider trying XSSH (page 22) instead, a locally developed variant designed to address just this problem.

Setup of SSH (and Troubleshooting)

SSH requires several careful, preliminary setup steps, and you must repeat these steps for every pair of (local and remote) machines between which you want to use SSH connections.

Basic Software Installation

In the unclassified environment (at LC or on any Internet site), to use SSH properly and to gain all the security advantages it offers (see above), you should run SSH on the machine on your desktop. SSH is available for Macintosh and Windows personal computers. If you have a UNIX workstation, your local administrator should install SSH on that machine. If you use an X terminal, SSH should be installed on the machine that supports your terminal sessions.

For help obtaining, installing, and configuring SSH clients on Macintosh computers, UNIX systems, or Windows machines, see the instructions and source links provided at this Open Lab Net web site (WARNING--SSH client files exceed 5 Mbyte, so they may download very slowly over telephone lines):

```
https://src.llnl.gov/software/ssh
```

An 89-page PDF-format SSH vendor's reference manual is also downloadable from this site. LLNL-specific initialization tips for UNIX machines appear in the next two sections. LLNL-specific installation tips for Macintosh computers also appear in a later section. (page 16) If you are not an LLNL employee covered by LLNL's site license for SSH, you can purchase your own copy from LLNL's vendor (Data Fellows) by contacting:

```
http://www.DataFellows.com/support/ssh
```

Until SSH is installed on your local machine you can still gain some security benefits by using SSH between LC hosts. The next two sections (below) apply to UNIX machines whether you are using SSH from your desktop or from one LC host to another. The "local" machine is always the one where you execute SSH; the remote or target machine is the system to which you want to connect using SSH.

Local Host Initialization (UNIX)

After SSH has been installed on the UNIX machine where you plan to run it, but before you can personally execute it, you must perform these initialization steps:

- Go to your home directory (type CD).
- If you have an old .ssh directory that has not been used, remove it using

  ```
  rmdir .ssh
  ```

- Run

  ```
  ssh-keygen
  ```

  and accept the default values it offers you by replying to each with a carriage return.
- When asked for a passphrase by SSH-KEYGEN, you may
  (1) enter a passphrase for extra security, or
  (2) enter a carriage return to use no passphrase.
  This passphrase has no connection to your LC log-on passwords.
  WARNING: a passphrase CANNOT be used if you plan to run SSH for noninteractive connections such as with PVM or batch-job submittals.
- Type

  ```
  ls -l .ssh
  ```

  to confirm the files automatically placed into your newly created .ssh directory:
  (1) IDENTITY.PUB contains your public key (a very long text line).
  (2) IDENTITY contains your private key, which is nonreadable data.
- Type

  ```
  ls -ld ~/.ssh
  ```

  to confirm that your .ssh directory has permissions RWX for you (as owner) alone (that is, 700 permission only). If not, set the permissions using

  ```
  chmod 700 .ssh
  ```

Target Host(s) Initialization (UNIX)

Decide which target (UNIX) host(s) you want to connect to when you run SSH on your local host. Then perform these initialization steps on EACH target host. (These steps enable SSH to use your password for authentication or to automatically use "RSA (passwordless) authentication" instead when LC allows it, within the OCf llnl.gov domain or among LC's own SCF production machines.)

- Log on to the target UNIX host.
- Check that your target home directory does not allow world or group WRITE access. Type

  ```
  ls -ld ~
  ```

  and look for W in the world and group (rightmost) permission triples. SSH will fail if world or group WRITE access is allowed here. Using

  ```
  chmod 755 ~
  ```

  for example, will eliminate world and group write access to your target home directory.
- For each target host that SHARES the same home directory as the local host where you run SSH (for example, the /g common home directory shared among all open LC hosts), perform these steps:

  (1) Type

  ```
  ls ~/.ssh/authorized_keys
  ```

  to see if an AUTHORIZED_KEYS file already exists.

  (2) If YES, type

  ```
  cat ~/.ssh/identity.pub >> ~/.ssh/authorized_keys
  ```

  to APPEND your IDENTITY.PUB file to the end of AUTHORIZED_KEYS.

  (3) If NO, type

  ```
  cp ~/.ssh/identity.pub  ~/.ssh/authorized_keys
  ```

  to CREATE an AUTHORIZED_KEYS file.

- For each target host that does NOT share the same home directory as your local host, perform these steps:

  (1) Type

  ```
  ls -la
  ```

  in your home directory to see if a .ssh directory already exists.

  (2) If NO, create one and set its required permissions:

  ```
  mkdir .ssh
  ```

  ```
  chmod 700 .ssh
  ```

  (3) If YES, set its required permissions:

  ```
  chmod 700 .ssh
  ```

  (4) Move (CD) into your .ssh directory and use LS to see if an AUTHORIZED_KEYS file already exits.

  (5) If NO, create one that contains the same unbroken long string that appears in your .SSH/IDENTITY.PUB file on your local machine. This is usually best done by running FTP and getting that file, with name changed to AUTHORIZED_KEYS when it arrives on the target machine:

  ```
  ftp your.local.host
  [log in as usual]
  binary
  get identity.pub authorized_keys
  quit
  ```

  (6) If YES, then move a copy of your local host's IDENTITY.PUB file to the target machine and APPEND it to the existing AUTHORIZED_KEYS file (do NOT simply replace that file, which may be accumulating keys from many different local hosts). First use FTP:

  ```
  ftp your.local.host
  [log in as usual]
  binary
  get identity.pub
  quit
  ```

  Then use CAT:

  ```
  cat identity.pub >> authorized_keys
  ```

REMINDER: You must repeat the whole sequence of steps in this section for every pair of local and target (UNIX) hosts between which you plan to use SSH (or SCP), as long as they do not share a common home (/g) directory.

Every LC production machine has a client and a server (daemon) for SSH2 as well as for SSH1 (the current default SSH). SSH2 and SSH1 do not share the same configuration files, however. So if you wish to use SSH2, see the SSH2 and DSA Authentication (page 18) section below for a parallel but separate set of instructions.

Troubleshooting SSH

Here are some common SSH problems and the suggested responses to them:

- NO DAEMON.
  You cannot use SSH to contact any host that is not already running the SSH daemon. Contact the host's system administrator (or the LC Hotline) if you think the daemon has not been installed.
- WRONG PERMISSIONS.
  Check that your target home directory does not allow world or group WRITE access; such access causes SSH to fail. (For example, 700 and 755 are compatible with using SSH, but 766 is not.) Use CHMOD to reset the faulty permissions.
- AUTHORIZATION FILE FLAWS.
  Check that the IDENTITY.PUB line was appended to the target host's AUTHORIZED_KEYS file as a single long line with no breaks. Careless editing can insert returns into this line, spoiling it.
- HOST KEY QUERY 1.
  If you attempt to connect to a target host using SSH and receive the message

  ```
  Host key not found from the list of known hosts.
  Are you sure you want to continue connecting (yes/no)?
  ```

  simply respond YES (warning: typing Y alone will be inadequate). SSH will update its list of known hosts (where it regards ILX1 and ILX1.LLNL.GOV as different machines).
- HOST KEY QUERY 2.
  If you attempt to connect to a target host using SSH and receive the message

  ```
  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  @       WARNING: HOST IDENTIFICATION HAS CHANGED!         @
  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
  Someone could be eavesdropping on you right now
  (man-in-the-middle attack)!
  Are you sure you want to continue connecting (yes/no)?
  ```

  simply respond YES and SSH will add another entry to your local ~/.ssh/known_hosts file. This message usually occurs because SSH considers ILX1 and ILX1.LLNL.GOV to be different machines, for example, despite your earlier successful setup work on a target host.
- OTHER PROBLEMS (VERBOSE MODE).
  You can always run SSH with the -v (verbose) option to gather additional troubleshooting clues. Or run the KLIST utility to report on the current status (expiration date, etc.) of your "kerberos authentication ticket."

Macintosh SSH Installation Tips

[Very similar steps and settings apply to installing SSH clients in a Windows environment.]

OBTAINING SSH.

You will need 3 Mbytes of free RAM, 2 Mbytes of free disk space, and MacTCP to use SSH on your Manintosh. LLNL employees who want to install SSH on an open Macintosh computer within the llnl.gov domain can get a site-licensed copy and an installer (helper) file for free by running a web browser (such as Netscape) on their Mac and opening this URL:

```
http://snd.llnl.gov/esdserver.html
```

This is an alphabetical "Electronic Software Distribution" list, with a "Secure Shell SSH" section. Clicking on the link labeled MacSSH101.sea.hqx

- downloads MacSSH (called F-secure SSH) and places its icon on your desktop display,
- downloads the installer for MacSSH as well, and places its separate icon on your desktop, and
- automatically expands these files with UnStuff.

INSTALLING SSH.

(1) Double click on the MacSSH Installer icon to begin.
(2) Read (or save to read later) the several scrolling screens of background advice that the installer presents. Then click CONTINUE.
(3) Select your choice from the offered alternatives EASY INSTALL (which is adequate) or CUSTOM INSTALL (more steps).
(4) Respond to the query "Do you want F-secure SSH to be able to run on all Macintosh computers" by clicking on NO (where YES is the default).
(5) At the message "installation was successful," click on QUIT.

CONFIGURING SSH.

When you first run SSH on your Macintosh, you must specify and then save several configuration choices, since many default session properties are inappropriate.
(1) Double click on the F-secure SSH icon.
(2) A greeting screen, then a small, untitled, empty terminal window appears.
(3) Press RETURN.
(4) A "Connect Using Password Authentication" dialog box appears.
(5) Skip the fill-in fields and instead click on the PROPERTIES button (right side) to specify and preserve your desired customizations.
(6) A file-folder image appears, with several labeled "tabs" across the top. For each tab listed in the chart below, supply the indicated information or select the indicated property (but do NOT click the OK button on any screen until all the tab screens listed here have been customized):

```
TAB          YOU                  YOU
NAME         SUPPLY               SELECT

Connection   Host name (e.g., ilx1.llnl.gov)
             User name (your LC login name)
             Port (use 922, not the default 22)

Font                              Name (e.g., Courier)
                                  Size (e.g., 18)*
                                  Text Color
                                  Background Color
                                  Disconnect Color

Terminal     Scroll Back Buffer   AUTOWRAP
             (number of lines)    DISPLAY STATUS LINE

Keyboard                          BACKSPACE SENDS DELETE
```

(*)Warning: the same font size applies to screen display and to printed output. You will probably need to use the PERCENTAGE adjustment feature of the FILE|PAGE-SETUP menu to indirectly make the printed size different than the screen size.

(7) After choosing all your customizations, then click OK on the last PROPERTIES subscreen.

(8) The "Connect Using Password Authentication" dialog box reappears with (only) the password field blank. Supply your password for the target host and click OK to begin your interactive SSH session with that host.

(9) While the session continues (and after confirming the appropriateness of your customizations), choose FILE|SAVE SETTINGS AS from the SSH menu bar. A dialog box appears and prompts for a "save as" name (e.g., ilx1.settings), which you supply. Click SAVE, and a new icon labeled with this string appears in your SSH folder. (To alter faulty customizations, select EDIT|CONNECTION PROPERTIES from the SSH menu bar to get the file-folder image again.)

RUNNING SSH.

(1) To return to a target host for which you have already saved SSH settings (using the configuration process above), double click on its labeled icon (within your SSH folder) and a customized terminal window will appear, with a password-prompting dialog box.

(2) To start a new SSH session from scratch, follow the configuration steps listed above.

SSH2 and DSA Authentication

Every LC production machine (OCF and SCF) has a client and a server (daemon) for SSH2 as well as for SSH1 (the current default SSH). Unfortunately, SSH2 and the default SSH1 do not share any of the same configuration files. In fact, SSH2 uses DSA authentication instead of RSA authentication (when allowed, within the llnl.gov domain on OCF and among LC's production machines on SCF). Secure FTP (SFTP) can use DSA authentication instead of one-time passwords (OTP) on OCF machines if you have enabled it.

To enable using SSH2 (and DSA authentication) on LC production machines, you can take advantage of the common home directory (one /g directory each on OCF and SCF) that all of these machines share to combine the "local" and "target" initialization steps into this single sequence:

- Go to your home directory on any LC production machine (type CD).
- If you have an old .ssh2 directory that has not been used, remove it using

  ```
  rmdir .ssh2
  ```

- Run

  ```
  ssh-keygen2
  ```

  and accept the default values it offers you by replying to each with a carriage return.
- When asked for a passphrase by SSH-KEYGEN2, you may
  (1) enter a passphrase for extra security, or
  (2) enter a carriage return to use no passphrase.
  This passphrase has no connection to your LC log-on passwords.
  WARNING: a passphrase CANNOT be used if you plan to run SSH2 for noninteractive connections such as with PVM or batch-job submittals.
- Type

  ```
  ls -l .ssh2
  ```

  to confirm the files automatically placed into your newly created .ssh2 directory:
  (1) ID_DSA_1024_A.PUB contains your public key (a very long text line).
  (2) ID_DSA_1024_A contains your private key, which is nonreadable data.
- Type

  ```
  ls -ld ~/.ssh2
  ```

  to confirm that your .ssh2 directory has permissions RWX for you (as owner) alone (that is, 700 permission only). If not, set the permissions using

  ```
  chmod 700 .ssh2
  ```

- Create the file ~/.ssh2/identification and insert a single line (IdKey id_dsa_1024_a) that points to your private key file. You can do this with any editor, or simply use ECHO:

  ```
  echo IdKey id_dsa_1024_a > ~/.ssh2/identification
  ```

- Create (or edit) the file ~/.ssh2/authorization and insert a single line (Key id_dsa_1024_a.pub) that points to your public key file. You can do this with any editor, or simply use ECHO:

```
echo Key id_dsa_1024_a.pub > ~/.ssh2/authorization
```

You are now enabled to use SSH2 and DSA authentication among all LC production hosts.

IPA Authorization for SSH

Starting on April 18, 2001, all offsite users (except for SNL and LANL users who start from their own restricted ("yellow") network) must first authenticate their session by using IP Port Allow (IPA) before they can connect to any LC machine, even by running SSH with port 922.

IP Port Allow (IPA) is an interactive, web-based process for registering the IP address of an outside-the-firewall computer for a specified period (8 hours by default) so that for that period the LLNL firewall allows SSH login service from that specific machine. LLNL employees, ASCI Alliance uses, and some other offsite users can establish an authorized IPA account by contacting the LC Hotline (paperwork and approvals required).

If you have an IPA account already, follow these steps to authenticate an SSH session:

(1) Use a web browser on your offsite machine to reach

`https://access.llnl.gov/ipa/login`

(note the s in https here).

(2) Confirm the name of your computer and then enter your IPA official ID (which is your PH-reported LLNL e-mail ID, NOT your LC login name) and your IPA password (which is now your LC authenticator-generated one-time password) in the form fields offered.

(3) Click SUBMIT. A confirmation that your address is IPA registered will appear. You can then exit the web browser if you wish.

(4) Run SSH (with port 922) to connect to your target LC machine; exit as usual when you are done with your interactive session.

(5) After your SSH connection closes, once again reach https://access.llnl.gov/ipa/login with a web browser. Change ALLOW to REMOVE on the login page, enter your IPA ID and password (OTP) again, and then click SUBMIT. This deactivates your IPA authentication.

Note that IPA autenticates a machine (really, the machine's IP address) for SSH use, not an individual user. If you share an offsite machine with other users, then the first user to authenticate with IPA has also enabled every user on the machine to successfully contact LC computers by running SSH (individual passwords are still required, of course). This shared authentication persists until its time limit is reached (the default is 8 hours) or until some user explicitly revokes it at LLNL's IPA login web site.

Using SSH (UNIX)

[Whenever you use an SSH client on an outside-the-firewall (outside llnl.gov) machine to connect to an LC OCF machine, remember to:
(1) first authenticate with IPA (page 20) before you execute SSH, and
(2) always use port 922 (-p 922) instead of the default port 22.]

When you log on to a (UNIX) machine using SSH, your customization (dot) files are executed just as they are at the start of a TELNET session. And you arrive in your home directory, just as you would have with TELNET. Your path and other environment variables are set by your dot files. If you do not specify a full pathname for a remote command, the value of $PATH is used for the search path. The default current location (invoked in a syntax such as ./myscript) is your home directory.

WARNING: When you execute a command remotely using SSH *without* logging in to the remote host, however, SSH (emulates RSH and) usually does *not* execute the command in a login shell. Usually, your customization (.login, .profile, etc.) files are *not* executed, so your environment variables (including PATH) are not set as they would be if you had logged in. This may cause your remote command to fail or misbehave. If you avoided logging in because of high interaction overhead and slow performance, consider using XSSH (page 22) instead (see the next section).

Here are some typical SSH execute lines, with explanatory comments. They are all shown in their most general form (which always works), but you can OMIT the special port request (-p 922) if you are:
(1) on an OCF machine within llnl.gov, or
(2) on an SCF LC production machine, or
(3) starting from an SNL or LANL restricted-access machine.

- Simple log on:

```
ssh -p 922 targethost
example: ssh -p 922 ilx1.llnl.gov
```

  (makes the current window a session on ILX1).

- Log on with different target user name:

```
ssh -p 922 -l LCusername targethost
example: ssh -p 922 -l arn ilx1.llnl.gov
```

  (local user arnold with LC username arn logs on to ILX1).

- Execute command on target host:

```
ssh -p 922 targethost targetcommand
example: ssh -p 922 ilx1.llnl.gov xterm
example: ssh -p 922 ilx1.llnl.gov ./myscript
```

  (runs the specified command as if you had logged on).

- Execute command on target host with different username:

```
ssh -p 922 -l LCusername targethost targetcommand
example: ssh -p 922 -l arn ilx1.llnl.gov xterm
example: ssh -p 922 -l arn ilx1.llnl.gov ./myscript
```

  (runs the specified command as if you had logged on as arn).

XSSH

ROLE.

XSSH is a locally developed (by AX Division) alternative to SSH designed to let you run a remote X client under conditions where regular SSH would yield results that were unreliable, unacceptably slow, or both. XSSH is on all LC OCF and SCF production machines.

When you use regular SSH not to log in to a remote machine but instead just to execute a remote X client there, the remote client does *not* usually execute in a login shell. Hence, your .login and .profile scripts on the remote machine never run, which in turn means that your remote environment variables are not set (or set improperly). The remote client often behaves badly as a result. If you compensate by using regular SSH to log in to the remote machine before running your desired X client there, part of the resulting (longer) communication path (the part between your local SSHD daemon/server and your local X server) is encrypted, and such encryption can cause very poor performance during high-traffic graphics or animation sessions. XSSH solves this specific problem (it still uses .Xauthority for strong security at login, but it eliminates the costly encrypted exchanges with SSHD).

PREREQUISITES.

To use XSSH you must meet three conditions:

- You must either use a UNIX (operating-system) computer (where an X server is normally available) or else execute an X-server application (such as Xwin32, Exceed, Exodus, or MacX) *before* you start your XSSH connection to a remote machine.
- PERL must reside on both the local and remote machines to sustain an XSSH connection between them. XSSH uses PERL to restart ~/.xboot (see next item) within a login shell on the remote host.
- The file ~/.xboot must reside in the home directory of every machine to which you want to make an XSSH connection. Since all LC production machines share a common home directory, you may be able to install this file just once (each on OCF and SCF). To install ~/.xboot in a machine's home directory, execute XSSH and invoke its special -xboot option:

  ```
  /usr/gapps/axdot/xssh -xboot
  ```

  Use SCP or FTP to move a copy of this file to any destination machine without a common home directory.

EXECUTE LINE.

After meeting its prerequisites (above), run XSSH by typing

```
/usr/gapps/axdot/xssh [options] [user@]host [command]
```

where

options	offer extra controls for a few specialized situations (along with -xboot, whose role was explained above). See /usr/local/docs/xssh_doc for option details.
user	specifies your login name on the remote machine (needed only if it differs from your login name on the local machine where XSSH runs).
host	specifies your intended remote target machine, as with regular SSH.

command is the X client that you want to run on the remote machine (default is XTERM, which opens a new terminal window to accept your further interactive commands). The long DOE legal warning and a few short messages from XSSH also appear when XTERM executes.

DETAILS.

For further technical details on how XSSH differs from SSH, for an option summary, and for troubleshooting tips on the most common pitfalls when using XSSH, consult the 180-line plain text file located on all LC production machines at

```
/usr/local/docs/xssh_doc
```

Virtual Private Network (VPN)

Virtual Private Network (VPN) is a way to temporarily borrow an llnl.gov IP address (from a pool for that purpose), so that while a VPN client runs on your outside-the-firewall machine all other applications there (such as your web browser or your FTP client, but not SFTP) perform with the same privileges that they would have if your computer were inside instead of outside the LLNL firewall.

Unlike IPA (page 20), VPN use requires that you download and install a VPN client on your machine and then execute it during every VPN authenticated session. Your VPN client interacts with a corresponding VPN server (vpn.llnl.gov) at LLNL while it runs. VPN clients for Macintosh, Windows, and UNIX platforms are available to authorized LC users for free download from https://access.llnl.gov/vpn, as noted in the next subsection. Only LLNL employees and certain other ASCI collaborators can establish an authorized VPN account, whose ID and password (NOT the same as your LC authenticator-generated one-time password) are required to run the VPN client, by contacting the LC Hotline (paperwork and approvals are required).

The subsections below tell how to get an appropriate VPN client for your outside-the-firewall machine, how to install and configure it, and how to run it to enable VPN-authorized use of your other programs.

Getting a VPN Client

VPN client executable files for Macintosh, Windows, and UNIX platforms (and for several variations of each operating system) are available to authorized users for free download from:

`https://access.llnl.gov/vpn/cgi-bin/vpn-client-check.cgi`

(Note the s in https here.) Offsite uses must already have an authorized VPN account so that they can provide their official VPN ID (not LC login name) and VPN password before the download begins (contact the LC Hotline to get an account). Onsite users will not be asked for authentication to download clients. The client files are only about 1 Mbyte, so if downloading directly to your offsite machine poses a problem, you could download the appropriate client to an LC machine and e-mail it to yourself as an attachment.

Installing and Configuring VPN

INSTALL.

To install your downloaded VPN client in either the Macintosh or Winndows environment, just double click on the downloaded executable file. This starts an installation wizard that leads you through several screens of set-up steps. After installation, the wizard offers to restart your computer, which is necessary to make VPN available for use.

CONFIGURE.

To configure the VPN client once installed, follow these steps:

- Start the VPN client by double clicking on its icon on your desktop (or otherwise finding and clicking on the VPN client where you have installed it).
- On VPN's displayed Configuration tab (top of window) click ADD.
- Set the Login Name to: your LLNL official ID (this is your PH-reported official e-mail name, NOT your LC login name).
- Set the Primary VPN Server to: vpn1.llnl.gov (128.115.248.42)
- Set the Secondary VPN Server to: vpn2.llnl.gov (128.115.248.43)
- Set Local Tunneling Control to: Tunnel IP (or click on Tunnel IP; note that this setting does NOT appear on all VPN clients).
- Click OK.
- Click Set [As] Default (note that this setting does NOT appear on all VPN clients).

Installation steps and needed configuration are now complete. See the next subsection for tips on routine use of VPN. (If you started VPN service before March, 2003, you may need to delete your old VPN Client Profile file and create a new one because the VPN server IP addresses changed at that time.)

Using VPN to Contact LLNL

Your local VPN client interacts with a VPN server at LLNL while it runs. So sometimes (unacknowledged) problems with the server will prevent you from successfully starting a VPN session. This is usually self-correcting, so just try again if your request for a connection is at first refused.

To use your VPN client (after installing and configuring it, above), follow these steps:

- Start the VPN client (find and double click on its icon).
- Click the CONNECT button.
- Complete the pop-up dialog box that appears:
  - ◊ For the Shared Secret enter: the string provided when you activated your VPN account (or contact your OISSO). Onsite uses can click here to see the string.
  - ◊ Click OK.
- If needed, complete the dial-up initiation box that may appear at this point (depends on your Internet service).
- Complete the second pop-up dialog box that appears:
  - ◊ For the Password, enter: your VPN password (now the same as your LC authenticator-generated one-time password).
  - ◊ For the Authentication Secret enter: the string provided when you activated your VPN account (or contact your OISSO). Onsite uses can click here to see the string.
  - ◊ Click OK.

After a few seconds, the status line at the bottom of the VPN client window will display one of several similar confirmation messages if a VPN session has successfully started:

```
     User xxx connected to vpn1.llnl.gov
or
     Connected to xxx@vpn1.llnl.gov [128.115.248.42]
```

After your VPN client confirms your connection to LLNL, leave it running throughout your session so that your borrowed llnl.gov IP address remains available to other programs. You can now run other applications (such as a web browser to access LLNL-only web sites) as you nornally would. All should behave as if your outside-the-firewall machine were within the llnl.gov domain (although web traffic to other, nonLLNL sites goes and comes directly to those sites, not by way of LLNL). Three warnings apply:
(1) If your web browser is configured to use a proxy server, then you must reconfigure it to NOT use a proxy server (just the reverse of the setting required for Web Proxy Service).
(2) If you are connecting back from LLNL (using X-windows, for example), then you must use the name that VPN temporarily assigns to your computer (of the form vpn###.llnl.gov). On the VPN client window, click on the LOGGING tab (along the top) to see a screen that reveals the current name or IP address (depends on client) assigned to your computer for this session.

(3) LC has confirmed that VPN enables inward file transfers with FTP (even to storage) when FTP and VPN run under Windows98, but you may encounter vendor-compatibility problems with other versions of Windows or with other operating systems.

To end your VPN-authorized session with LLNL, follow these steps:

- Exit all the application programs that depend on VPN authorization to work properly.
- On the VPN client Configuration tab, click DISCONNECT (not available on all VPN clients).
- Click EXIT.

Disclaimer

Keyword Index

To see an alphabetical list of keywords for this document, consult the next section (page 30).

Alphabetical List of Keywords

Keyword	Description
a	The alphabetical index of keywords.
availability	Where these programs run.
cryptocards	Former cryptocard status.
date	The latest changes to this document.
entire	This entire document.
firewall-features	Diagram and analysis of LC firewall.
ftp	FTP blocked inbound; alternatives.
index	The structural index of keywords.
installation	SSH installation advice (UNIX).
introduction	Background terms and distinctions.
local-init	Initializing SSH on a local host.
revisions	The complete revision history.
scope	Topics covered in this document.
services	Instructions for firewall-altered services.
ssh	Secure shell (SSH) instructions.
ssh-execute-line	Typical SSH execute lines.
ssh-ipa	Offsite IPA authentication for SSH.
ssh-macintosh	Special steps for SSH Mac installations.
ssh-role	What SSH does.
ssh-setup	How to set up SSH.
ssh2	Set up for SSH2 and DSA (optional).
target-init	Initializing SSH on a target host.
telnet	TELNET blocked inbound; alternatives.
title	The name of this document.
troubleshooting	Common SSH problems addressed.
vpn	Virtual Private Network instructions.
vpn-client	How to get a VPN client.
vpn-config	How to install, configure VPN client.
vpn-usage	How to routinely use VPN connections.
who	Who to contact for assistance.
xssh	Low-overhead local alternative to SSH.

Date and Revisions

Revision Date	Keyword Affected	Description of Change
15Sep03	xssh	New section, local alternative.
	ssh-role	Cross ref to XSSH added.
	ssh-execute-line	Environment variable warning added.
	index	New keyword for new section.
01Apr03	vpn	Primary, secondary servers explained.
	ssh-ipa	IPA now uses OTP.
	firewall-features	Two VPN servers noted.
12Feb03	firewall-features	SFTP service added.
	ftp	Comparison with SFTP added.
	ssh2	DSA authentication for SFTP ok.
	ssh-execute-line	ILX replaces LX in all examples.
25Mar02	scope	Cross ref. added for EZSTORAGE.
	ftp	Former machines no longer exist.
10Dec01	ssh2	New section on SSH2 and DSA.
	ssh-setup	RSA aspects clarified.
	ssh-execute-line	When to use -p 922 clarified.
	index	New keyword for new section.
08Oct01	ftp	Anonymous FTP at ftp.llnl.gov only.
	ssh-role	SSH now OTP enabled (OCF).
	ssh-ipa	IPA password is not OTP.
	vpn	VPN password is not OTP.
09Apr01	vpn	New section explains VPN role, use.
	ssh-ipa	New section on IPA authentication of SSH.
	firewall-features	VPN added, SSH changed for IPA.
	ftp	VPN enables FTP through firewall.
	ssh	Technical updates (port 922, IPA).
	index	New keywords for new sections.
06Feb01	firewall-features	TELNET among LC hosts blocked.
	telnet	TELNET among LC hosts blocked.
	ftp	Annonymous FTP clarified.
	ssh-role	More TELNET blocking noted.
10Apr00	entire	Gateway, CRYPTOCards disabled. All sections revised.
25May99	firewall-features	TELNET blocking scope expanded.
	telnet	TELNET blocking scope expanded.

10May99	ssh-role	Data encryption clarified.
	ssh-setup	UNIX aspects clarified.
	ssh-macintosh	New Mac instructions added.
	index	New keyword added.
23Feb99	ftp	Firewall blocking enabled.
	firewall-features	FTP blocking enabled.
	ssh-setup	Another SSH source added.
25Jan99	entire	First edition of Firewall/SSH manual.

TRG (15Sep03)

UCRL-WEB-201524

TRG (15Sep03) Contact on the OCF: lc-hotline@llnl.gov, on the SCF: lc-hotline@pop.llnl.gov